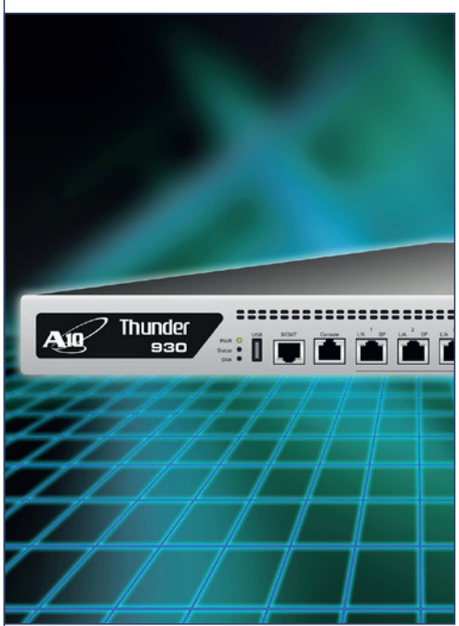
Verfügbare Applikationen als Selbstverständlichkeit

Die Sicherstellung einer maximalen Verfügbarkeit und Sicherheit unternehmenskritischer Anwendungen ist ein anspruchsvolles Unterfangen. UASGs (Unified Application Service Gateways) leisten dazu einen wichtigen Beitrag – für ISPs, Carrier, Enterprises und KMU gleichermassen.

Server Load Balancer (SLB) und Application Delivery Controller (ADC) kommen dann zum Tragen, wenn es gilt, Anwendungen schneller, besser und sicherer bereitzustellen. Nebst dieser Kernaufgabe unterstützen sie in der Regel Funktionen wie Datenbank-Load-Balancing und Lastverteilung auf mehrere Firewalls. Die beeindruckende Performance führender Systeme erlaubt nun die Erweiterung zu sogenannten «Unified Application Service Gateways» (UASG). Dabei handelt es sich um ADCs mit markant erweiterten Security- und Networking-Funktionen. Verfolgt wird dabei das Ziel, wesentliche Security-Funktionen so nahe wie möglich am Perimeter beziehungsweise am äussersten Punkt des Firmengateways anzusiedeln. Denn Schadcode, der bereits am Perimeter beziehungsweise vor der Firewall abgewehrt wird, verhindert eine unnötige Belastung und Gefährdung der internen IT- und Netz-Infrastruktur.

Security am Firmengateway

Um einen maximalen Perimeterschutz zu gewährleisten, unterstützen die Unified Application Service Gateways von A10 Networks die Funktionen Web Application Firewall (WAF) und DNS Application Firewall. WAFs haben zur Aufgabe, Web-Anwendungen vor Angriffen via HTTP zu schützen, Code-Schwachstellen zu sichern und Datenverluste zu verhindern. UASGs mit WAF-Funktion sind demnach in der Lage, Angriffe auf Webserver zu erkennen und abzuwehren. DNS Application Firewalls dienen dem Schutz von DNS-Infrastrukturen. Dabei gilt es, selbst massive Attacken ohne Belastung der DNS-Server wirksam abzuwehren. Als weiteres Leistungsmerkmal beinhalten UASGs ein Application Access Management (AAM). Diese integrierten Authentifizierungs-Funktionen stellen sicher, dass die Backend-Server keinen unerwünschten oder nicht authentifizierten Datenverkehr erhalten. Um einen wirksamen Schutz vor mehrschichtigen Distributed-Denial-of-Service-(DDoS-)Attacken zu etablieren, kombinieren die Appliances zudem mehrere Abwehrmechanismen wie SYN-Flood-Protection (stellen 25 Prozent aller DDoS-Zwischenfälle dar), geografische Filterung, Raten- und Verbindungslimitierung, «Slow HTTP»-Angriffserkennung, aFleX-Kommandos.



Unified Application Service Gateways (UASG) von A10 Networks maximieren die Verfügbarkeit von Applikationen, sorgen für Sicherheit am Gateway und ermöglichen eine nahtlose IPv6-Migration. Bild: A10 Networks

Server und Netzwerk ohne Leistungseinbussen

Um Applikationsserver und Netzwerk-Infrastrukturen zu entlasten, übernehmen UASGs rechenintensive Aufgaben und sorgen mit intelligenten Mechanismen dafür, dass der Datenverkehr reduziert wird. Mittels Komprimierung des HTTP-Protokolls beispielsweise reduzieren sie das Datenvolumen und die benötigte Bandbreite um Faktoren. Performancesteigernd wirkt ferner das sogenannte Traffic Caching, bei dem die Anzahl Verbindungen zum Server minimiert wird. Werden zudem mehrere HTTP-Verbindungen zu einer TCP-Sitzung zusammengefasst (TCP-Connection-Reuse), führt dies zu einer weiteren Entlastung von Server und Netzwerk. Ebenso effektvoll ist die mit SSL-Offloading bezeichnete Terminierung verschlüsselter Client-Verbindungen. Zudem lassen sich mit Hilfe von SSL-Bridging verschlüsselte Daten auf fehlerhaften Code überprüfen – bevor dieser den Server erreicht. Dazu wird der Code entschlüsselt, auf Inhaltsebene analysiert, neu verschlüsselt und an den Server weitergereicht. Dieser in beide Richtungen durchlaufende Prozess ist ohne hardwarebeschleunigte UASG kaum denkbar oder hätte markante Leistungseinbussen zur Folge.

Software Defined Networking (SDN) und IPv6-Migration

Zwei weitere, höchst aktuelle Themen – Software Defined Networking und IPv6-Migration – erhalten dank UASGs eine perfekte Grundlage. Einerseits ermöglichen Unified Application Service Gateways, das Netzwerk auf Basis von Informationen auf Applikationslayer-Ebene zu kontrollieren und auf diesem Weg die Anwendungsperformance zu optimieren. Andererseits ermöglichen sie eine uneingeschränkte Konvergenz zwischen IPv4 und IPv6 sowie eine nahtlose Migration auf IPv6.

DER AUTOR

Walter Benz,
Product Manager
A10 Networks,
Boll Engineering